ISSN 2424-5631 (online)

CYBER RISK INSURANCE – THE EMERGING PART OF NON-LIFE INSURANCE MARKET

Julija Gavėnaitė-Sirvydienė

Mykolas Romeris University, Lithuania
julija.gavenaite@gmail.com

Abstract

Purpose-to clarify the definition and characteristics of cyber risk and cyber insurance. More specifically to identify key parts of cyber insurance contract and analyse nowadays cyber insurance market.

Design/methodology/approach: analyse and study of scientific literature, analyse of statistics databases, data comparison.

Findings: firstly, this research paper provides an explicit definition of a cyber risk and cyber insurance. In general, financial institutions and regulators of insurance market categorize cyber type risks as a part of operational risk because it is related to technology and information assets. Therefore, cyber risk is described as operational risk that affects technology assets, information, databases and other sensitive online storage. According to guidelines provided in Solvency II and Basel II documents, cyber risks can be put into four categories: technology and system failures, unsuccessful internal processes, act of people, external processes. These four categories of potential cyber risks are described particularly in this article. Secondly, the comprehensive cyber insurance market analyses is provided following the article. According to AXA Insurance Solutions company there was 170 insurers offering cyber liability policies in 2017 and about 30 more new carriers joined the market in 2018. According to the Cyber Policy Inc. the number 5 cyber insurance carriers in the marker is: AIG; Chubb; Hiscox, Liberty Mutual, HSB. With the beginning of 2019 it is expected from buyers to keep pressuring the insurance companies to deliver even more comprehensive services, more coverage options and potential. In general, cyber insurance market is supposed to remain stable, but the quality of policy language should evolve together with other endorsements to general cyber insurance policy. Thirdly, the general guidelines of underwriting the cyber insurance coverage policy is provided within this paper. In order to implement any form of risk reduction for cyber risk (also including insurance), the company at first should very clearly expose its potential vulnerabilities and weaknesses. Three types of general internal company's

ISSN 2424-5631 (online)

information can be marked out for preparing the cyber insurance coverage background: IT related information; human resources; finance, internal audit, legal issues. For insurance company to better understand the company the general business information is most important part. In order to extent the company's disclosure to cyber threats and to better prepare the solutions if insurance this business profile information should be conducted very carefully. Prevention is one of the most important factors of a cyber risk insurance policy. Companies that are buying cyber risk insurance may get access to pre-breach assessments, prevented suppliers or cybersecurity information for this purpose.

Research limitations: this research paper concentrates on the European Union insurance market and experience of the insurer located in the EU. Moreover, this field of research is very unstable and the changing very fast together with continuously development of IT services sector. More studies and analyses should be made together with the changing environment of cyber security.

Practical implications: this research paper may serve not only for further studies and scientific discussion. Moreover, it could be useful for the businesses as a valuable tool to better understand what cyber insurance is, how to prepare for implementing cyber security policy in the company.

Keywords: insurance, risk management, business, cyber security, cyber insurance policy, cyber insurance market.

Research type: research paper